IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Alexandria Rudolph, individually and on behalf of all others similarly situated, Plaintiff, v. Hudson's Bay Company, a Canadian corporation; Saks Fifth Avenue LLC, a Massachusetts limited liability company; Saks & Company LLC, a Delaware limited liability company; Saks Incorporated, a Tennessee corporation, Lord & Taylor LLC, a Delaware limited liability company, Defendant(s).	Civil Action No. 1:18-cv-8472 (PKC) **SECOND AMENDED COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Alexandria Rudolph ("Plaintiff"), by and through her counsel, brings this Second Amended Class Action Complaint against Defendants Hudson's Bay Company ("HBC"), Saks Fifth Avenue LLC, Saks & Company LLC, Saks Incorporated (collectively "Saks"), and Lord & Taylor LLC (all entities are herein collectively referred to as, "Defendants") on behalf of herself and all others similarly situated, and alleges upon personal knowledge as to her own actions, and upon information and belief as to counsel's investigations and all other matters as follows:

NATURE OF THE ACTION

1. Plaintiff brings this consumer class action against Defendants for their failure to secure and safeguard their customers' credit and debit card numbers, which Defendants collected at the time Plaintiff and other Class members[1] made purchases at Defendants' Saks Fifth Avenue,

[1] Classes defined *infra* in Paragraphs 103-108.

Lord & Taylor, and Saks OFF 5TH stores ("Customer Data"), and for failing to provide timely, accurate and adequate notice to Plaintiff and Class members that their Customer Data had been stolen, as well as precisely what types of information were stolen.

2. On March 28, 2018, the notorious hacking group known as JokerStash (also known as "Fin7") announced the successful data breach of an unnamed major corporation, resulting in the unauthorized release of over five million stolen credit and debit cards.[2]

3. Subsequently, on April 1, 2018, the cyber-threat research group Gemini Advisory, working with several large financial institutions, confirmed that the stolen Customer Data belonged to HBC (hereinafter, the "Gemini Report").[3] HBC is the ultimate parent company for each of the Defendants and owns the Saks and Lord & Taylor stores ("HBC stores").

4. According to Gemini's Chief Technology Officer, the hack "penetrated the retailers' point of sale ["POS"] systems."[4] POS systems store highly-sensitive consumer data. Specifically, POS systems store "Track 1" and "Track 2" data from the magnetic strip on the payment card, which include at least the cardholder's first and last name, the expiration date of the card, and the CVV (three or four number security code on the card).[5] This data is among the information Fin7 stole from HBC, as demonstrated by Fin7's advertisement that the stolen information offered for sale includes "TR2+TR1" data.[6]

5. The Gemini Report confirmed that the breach occurred from approximately May

---

[2] Gemini Advisory, *Fin7 Syndicate Hacks Saks Fifth Avenue and Lord & Taylor Stores* (April 1, 2018), *available at* https://geminiadvisory.io/fin7-syndicate-hacks-saks-fifth-avenue-and-lord-taylor/ (last visited November 12, 2018).
[3] *Id.*
[4] Robert McMillan and Suzanne Kapner, *Saks, Lord & Taylor Hit With Data Breach* (Apr. 2, 2018), *available at* https://www.wsj.com/articles/saks-lord-taylor-hit-with-data-breach-1522598460 (last visited November 12, 2018).
[5] SLAVA GOMZIN, HACKING POINT OF SALE: PAYMENT APPLICATION SECRETS, THREATS, AND SOLUTIONS 98-103 (Carol Long ed. 2014)
[6] Gemini Advisory, *Fin7 Syndicate Hacks Saks Fifth Avenue and Lord & Taylor Stores* (April 1, 2018), *available at* https://geminiadvisory.io/fin7-syndicate-hacks-saks-fifth-avenue-and-lord-taylor/ (last visited November 12, 2018).

2017 to March 2018.

6. Following the Gemini Report, HBC confirmed that certain Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor stores in North America were subject to a data breach.[7]

7. Notably, while the Gemini Report calculated that the breach was active since May 2017, HBC's CEO asserted in an April 2018 "Notice of Data Breach" letter that the "malware began running" on its POS systems "around July 1, 2017".[8] Therefore, consumers who have made purchases at HBC stores between May and July 1, 2017 may not be on notice that their payment cards were, and continue to be, at risk.

8. The private Customer Data obtained from the data breach was compromised due to Defendants' acts and omissions and their failure to properly protect the Customer Data.

9. Defendants' failure to adequately protect Customer Data was not isolated to the 2017-2018 breach. Rather, in March 2017, HBC inadvertently "exposed the personal information of tens of thousands of [Saks Fifth Avenue] customers through the company's websites" to the public.[9]

10. In addition to Defendants' failure to prevent the data breach, they also failed to detect the breach for more than eleven months, only making a public statement regarding the breach after the Gemini Report.[10]

11. Defendants disregarded Plaintiff's and Class members' rights by intentionally,

---

[7] Hudson's Bay Company, http://investor.hbc.com/releasedetail.cfm?ReleaseID=1062423 (April 1, 2018) (last visited November 12, 2018).
[8] Hudson Bay Company, *Notice of Data Breach* (April 27, 2018), *available at* https://www.oag.ca.gov/system/files/HBC%20-%20Copy%20of%20Notice%20Materials_0.pdf (last visited November 12, 2018).
[9] Scott Eells, *Hudson's Bay exposes Saks customer info online* (March 20, 2017), *available at* https://www.theglobeandmail.com/report-on-business/hudsons-bay-exposes-saks-customer-info-online/article34346027/ (last visited November 12, 2018).
[10] Jim Finkle and David Henry, *Saks, Lord & Taylor hit by payment card data breach* (April 3, 2018), *available at* https://www.reuters.com/article/legal-us-hudson-s-bay-databreach/saks-lord-taylor-hit-by-payment-card-data-breach-idUSKCN1H91W7 (last visited November 12, 2018).

willfully, recklessly, or negligently failing to take adequate and reasonable data-security measures to ensure their data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to monitor and detect the breach on a timely basis, and failing to disclose to their customers the material facts that they did not have adequate computer systems and security practices to safeguard Customer Data.

12. If Defendants had maintained and implemented proper data-security measures to safeguard Customer Data, deter Fin7 and other hackers, and detect the breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented, or at the very least, its harm mitigated.

13. The data breach was the inevitable result of Defendants' inadequate approach to data security and the protection of the Customer Data that they collected during the course of their business. The deficiencies in Defendants' data security were so significant that the malware installed by the hackers remained undetected and intact for approximately one year.

14. The susceptibility of POS systems to malware is well-known throughout the retail industry. In the last five years, practically every major data breach involving retail store chains has been the result of malware placed on POS systems. Accordingly, data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[11]

15. HBC also recognized the risk of a consumer data breach in its Annual Information Form in April 2017, two months before Fin7 successfully breached Defendants' security systems. As HBC admits, "[a] potential privacy breach could have a material adverse effect on our business

[11] Datacap Systems Inc., *Point of sale security: Retail data breaches at a glance*, *available at* https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance# (last visited November 12, 2018).

and results of operations."[12] HBC further recognized that "[o]ur security measures may be undermined due to the actions of outside parties, employee error, malfeasance, and, as a result, an unauthorized party may obtain access to our data systems and misappropriate business and personal information."[13]

16. Indeed, Defendants failed to take steps to employ adequate security measures despite recent, well-publicized data breaches at large national retail chains, including Brooks Brothers, Kmart, Target, and Home Depot. Furthermore, Defendants exacerbated the situation by failing to detect the data breach earlier. Unfortunately, Defendants' profit-driven decisions to ignore these warning led to the damage upon which this case is based. Had Defendants detected the breach earlier, less data would have been stolen and customers would have been able to take earlier action to mitigate their damages.

17. As a result of the data breach, Class members' Customer Data has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members as a direct result of Defendants' data breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a

[12] Hudson Bay Company, Annual Information Form, at 61 (Apr. 28, 2017).
[13] *Id.*

result of fraudulent charges stemming from the data breach including but not limited to foregoing cash back rewards;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet black market;

h. damages to and diminution in value of their Customer Data entrusted to Defendants for the sole purpose of purchasing products and services from Defendants and with the mutual understanding that Defendants would

safeguard Plaintiff's and Class members' data against theft and not allow access to and misuse of their information by others;

i. money paid for products and services purchased at Defendants' stores during the period of Defendants' data breach, in that Plaintiff and Class members would not have shopped at Defendants' stores had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' Customer Data; and

j. continued risk to their Customer Data which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in their possession.

18. The injuries to the Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for Customer Data.

19. Plaintiff and members of the Classes retain a significant interest in ensuring that their Customer Data, which remains in Defendants' possession, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose Customer Data was stolen as a result of the data breach.

20. Plaintiff, on behalf of herself and similarly situated consumers, seeks to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the data breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

THE PARTIES

21. Plaintiff Alexandria Rudolph is a resident of Los Angeles, California and was a California resident during the period of the data breach. On November 23, 2017, Plaintiff purchased items at a Saks OFF 5TH retail store located at 100 N La Cienega Blvd., Beverly Hills, California, with her Visa debit card, which was swiped through their point-of-sale payment device.

22. On May 18, 2018, Bank of America notified Plaintiff of suspected fraudulent activity on the Visa debit card Plaintiff used during her November 2017 purchase at the Saks OFF 5TH retail location. As a result, Bank of America froze Plaintiff's account associated with the payment card. Plaintiff's payment card was compromised despite Plaintiff having physical possession of her payment card at all times. Following the hold placed on her account, Plaintiff spent approximately 20 minutes contacting Bank of America telephonically attempting to resolve the issue. Because Plaintiff needed a new debit card immediately, Plaintiff drove approximately 25 miles, which took her about one and a half hours, to visit a Bank of America branch in person to get a new card. In doing so, Plaintiff expended cash in the form of gasoline expended to get to the bank. Specifically, Plaintiff used approximately 1.20 gallons of gasoline driving to the bank, which cost her approximately $4.68. At the bank, Plaintiff spent approximately 30 minutes discussing the account freeze with a banker and requesting and obtaining a new debit card. Plaintiff also spent approximately one hour looking through her account records after the account freeze. Further, since May 2018, Plaintiff has expended approximately 30 minutes in total updating her payment card information with various retailers. Finally, since May 2018, Plaintiff has spent several hours reviewing monthly financial statements for any fraudulent or suspicious charges. Plaintiff would not have spent this time and money otherwise had it not been for the data breach.

23. Plaintiff would not have used her debit card to make purchases at Saks —indeed, she would not have shopped at Saks at all during the period of the HBC data breach—had Defendants told her that they lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

24. Plaintiff suffered actual injury from having her Customer Data compromised and stolen in and as a result of the data breach.

25. Plaintiff suffered actual injury and damages in paying money to and purchasing products from Saks during the data breach that she would not have paid had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' Customer Data.

26. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Customer Data – a form of intangible property that she entrusted to Defendants for the purpose of purchasing their products and that was compromised in and as a result of the data breach.

27. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her Customer Data being placed in the hands of criminals who have already misused such information stolen in the data breach via the sale of Plaintiff's and Class members' Customer Data on the Internet black market. Plaintiff has a continuing interest in ensuring that her private information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

28. Plaintiff is likely to purchase items from Defendants' stores with a credit or debit card in the future if their data security was improved to protect against future data breaches.

29. Defendant Hudson's Bay Company is a Canadian corporation and maintains its U.S. headquarters, and main base of operations, in New York, New York.

30. Defendant Saks Fifth Avenue LLC is a Massachusetts limited liability company with its principal place of business in New York, New York. The sole member of Saks Fifth Avenue LLC is Saks & Company LLC, a Delaware limited liability company.

31. Defendant Saks & Company LLC is a Delaware limited liability company with its principal place of business in New York, New York. Defendant Saks & Company LLC maintains its support operations in Jackson, Mississippi, including functions such as accounting, credit card administration, and information technology. For example, Defendant maintains its primary support operation center in Jackson, Mississippi, which processes and tracks every point-of-sale transaction for Saks OFF 5TH locations.[14] The sole member of Saks & Company LLC is Saks Incorporated, a Tennessee corporation.

32. Defendant Saks Incorporated is a Tennessee corporation with its principal place of business in New York, New York.

33. Defendant Lord & Taylor LLC is a Delaware limited liability company with its principal place of business in New York, New York. The sole member of Lord & Taylor LLC is Lord & Taylor Holdings LLC, a Delaware limited liability company with its principal place of business in New York, New York. The sole member of Lord & Taylor Holdings LLC is Lord & Taylor Acquisition Inc., a Delaware corporation.

[14] Wally Northway, *Saks Operations Center Committed* To Jackson (July 2, 2007), *available at* http://msbusiness.com/2007/07/saks-operations-center-committed-to-jackson/ (last visited November 12, 2018).

34. HBC's operates 48 Lord & Taylor stores, 42 Saks Fifth Avenue stores, and 132 Saks OFF 5TH stores.[15] Defendants' retail stores accept payment for their goods and services through a POS system, through which customers use credit and debit cards to pay.

JURISDICTION AND VENUE

35. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

36. This Court has personal jurisdiction over Defendants because Defendants conduct substantial business in New York, including this District, and have sufficient minimum contacts in New York. This Court also has general jurisdiction over Defendants because each Defendant maintains its principal place of business in this District.

37. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because all Defendants maintain their principle place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2).

STATEMENT OF FACTS

A. History and Customer Data Collection Practices

38. HBC was founded in 1670 and is Canada's largest diversified general merchandise retailer, operating more than 480 stores worldwide. In 2017, HBC produced global sales of more than $14 billion.[16]

[15] Hudson Bay Company, Management's Discussion and Analysis of Financial Condition and Results of Operations for the Thirteen and Twenty-Six Weeks Ended August 4, 2018, at 16.
[16] *Available at* https://www.marketwatch.com/investing/stock/hbc/financials. (last visited November 12, 2018).

39. HBC serves as the parent company for the Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores ("HBC stores"), acquiring the Saks Fifth Avenue brand in 2013.[17]

40. With its "soaring profits and revenues", HBC heavily invested in the remodeling of its stores and upgrades to its distribution and fulfillment centers, with "[o]ne of the company's biggest growth initiatives this year involve[ing] expanding the Saks Off 5th [. . .] footprint."[18] In fact, "[r]oughly 30% of the capital budget allocated to growth initiatives will be spent on 32 new Off 5th stores and seven new full line Saks stores" and the "number of Saks Off 5th stores will surge dramatically as will investment in technology. . . ."[19] Despite these substantial investments to upgrade the appearance and technology of their stores to boost sales, Defendants failed to make meaningful improvements to its data security systems, including its POS systems, placing customer's Customer Data at risk.[20]

41. A significant portion of these sales at Defendants' stores are made to customers using credit or debit cards. When Defendants' customers pay using credit or debit cards, Defendants collects Customer Data related to those cards including the cardholder name, the account number, expiration date, and card verification value (CVV). Defendants store the Customer Data in their POS system and transmits this information to a third party for completion of the payment.

---

[17] Michelle da Silva, *Hudson's Bay Company Acquires Saks Fifth Avenue* (Nov. 4, 2013), available at https://www.straight.com/news/522951/hudsons-bay-company-acquires-saks-fifth-avenue. (last visited November 12, 2018).

[18] Mike Troy, *Surging Hudson's Bay Details Major Investments in Expanding Saks, Saks Off 5th and Store Renovation* (April 5, 2016), available at https://www.chainstoreage.com/article/surging-hudsons-bay-details-major-investments-expanding-saks-saks-th-and-store-renovations/ (last visited November 12, 2018).

[19] *Id.*

[20] On information and belief, Defendants contracted with various third parties to install, manage, service and maintain the POS equipment and software who may also be responsible or liable for allowing the hackers to gain access and deploy malware on the POS systems in Defendants' network. Plaintiff hereby provides Notice that after discovery, she may seek leave to add those third-party vendors as party defendants in this litigation.

42. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Customer Data they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

43. Stolen Customer Data is a valuable commodity. A "cyber black-market", such as the one used by Fin7, exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. The Customer Data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

44. Legitimate organizations and the criminal underground alike recognize the value in Customer Data contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it.

45. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on their customers as a result of a breach.

46. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions at their North American retail locations, amounting to a large volume of daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

47. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of Customer Data in the hands of other third parties, such as other nationwide retailers, Defendants' approach to maintaining the privacy and security

of the Plaintiff's and Class members' Consumer Data was lackadaisical, cavalier, reckless, or at the very least, negligent.

B. Defendants Had Notice of Data Breaches Involving Malware on POS Systems

48. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[21] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[22] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[23]

49. Most of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants. A POS system is an on-site device, much like an electronic cash register, which manages transactions from consumer purchases, both by cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[24] The payment processor then passes on the payment information to the financial institution that issued the card and takes the other steps needed to complete the transaction.[25]

---

[21] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), available at https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last visited November 12, 2018).
[22] *Id*.
[23] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), *available at* https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited November 12, 2018).
[24] *Id.* at 6.
[25] Gomzin, *supra* note 5, at 8-9.

50. Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory.[26] The stored information includes "Track 1" and "Track 2" data from the magnetic strip on the payment card, such as the cardholder's first and last name, the expiration date of the card, and the CVV (three or four number security code on the card).[27] This information is unencrypted on the card and, at least briefly, will be unencrypted in the POS terminal's temporary memory as it processes the data.[28]

51. According to Gemini's Chief Technology Officer, the hack "penetrated the retailers' point of sale ["POS"] systems."[29] This data is among the information Fin7 stole from HBC, as demonstrated by Fin7's advertisement that the stolen information offered for sale includes "TR2+TR1" data.[30]

52. In order to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration and aggregation.[31] In the infiltration phase, an "attacker gains access to the target environment"[32] allowing the hackers to move through a business's computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[33] Once inside the system the attacker then infects the

[26] Symantec, *supra* note 23, at 6.
[27] Gomzin, *supra* note 5, at 98-103.
[28] Symantec, *supra* note 23, at 5.
[29] Robert McMillan and Suzanne Kapner, *Saks, Lord & Taylor Hit With Data Breach* (Apr. 2, 2018), *available at* https://www.wsj.com/articles/saks-lord-taylor-hit-with-data-breach-1522598460 (last visited November 12, 2018).
[30] *Id.*
[31] *Point of Sale Systems and Security: Executive Summary*, SANS Institute, 4 (Oct. 2014), *available at* https://www.sans.org/reading-room/whitepapers/analyst/point-salesystems-security-executive-summary-35622 (last visited November 12, 2018).
[32] *Id.*
[33] Symantec, *supra* note 23, at 6.

POS systems with malware, which "collects the desired information . . . and then exfiltrates the data to another system" called the "aggregation point."[34]

53. A 2016 report by Verizon confirmed "[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data."[35] According to Verizon, hackers successfully compromise POS systems in a matter of minutes or hours and exfiltrate data within days of placing malware on the POS devices.[36]

54. Intruders with access to unencrypted Track 1 and Track 2 payment card data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[37] Since 2014, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet.[38] In 2015, intrusions into POS systems accounted for 64% of all breaches where intruders successfully stole data.[39] For example, in 2013, hackers infiltrated Target, Inc.'s POS system, stealing information from an estimated 40 million payment cards in the United States.[40] In 2014, over 7,500 self-checkout POS terminals at Home Depots throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[41]

---

[34] *Id*.
[35] *Id*.
[36] *Id*. at 4.
[37] *Id.* at 3.
[38] *See, e.g., 2016 Data Breach Investigations Report*, Verizon, at 1 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, available at (last visited November 12, 2018).
[39] *Id*. at 3.
[40] https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ (last visited November 12, 2018).
[41] Brett Hawkins, *Case Study: The Home Depot Data Breach,* 7 (SANS Institute, Jan. 2015), *available at* https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367 (last visited November 12, 2018).

55. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, Defendants were aware or should have been aware of the need to safeguard their POS systems.

C. Defendants Failed to Comply with Industry Standards

56. Despite the vulnerabilities of POS systems, available security measures and reasonable business practices would have significantly reduced or eliminated the likelihood that hackers could successfully infiltrate the business' POS systems. One report indicated that over 90% of the data breaches occurring in 2014 were preventable.[42]

57. The payment card networks (MasterCard, Visa, Discover, and American Express), data security organizations, state governments, and federal agencies have all implemented various standards and guidance on security measures designed to prevent these types of intrusions into POS systems. However, despite Defendants' understanding of the risk of data theft via malware installed on POS systems, the widely available resources to prevent intrusion into POS data systems, and Defendants' previous public display of customer's private information, Defendants failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Data Breach.

58. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, more than two years ago, Symantec recommended "point to point encryption" implemented through secure card readers, which encrypts credit card information in the POS system, preventing malware that extracts card information through the POS memory while it processes the transaction.[43] Moreover, Symantec emphasized the

[42] Verizon, *supra* note 38, at 1.
[43] Symantec, *supra* note 23, at 6.

importance of adopting EMV chip technology. Last year, Datacap Systems, a developer of POS systems, recommended similar preventative measures.[44]

59. The major payment card industry brands set forth specific security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

60. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.[45]

61. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[46] PCI DSS sets the minimum level of what must be done, not the maximum.

62. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, imposes the following mandates on Defendants:[47]

[44] *See* Datacap Systems, *supra* note 11.
[45] *Payment Card Industry Data Security Standard* v3.2, at 5 (Apr. 2016), *available at* https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited November 12, 2018).
[46] *Id*.
[47] *Id*.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

63. Among other things, PCI DSS required Defendants to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

64. PCI DSS also required Defendants to not store "the full contents of . . . the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[48]

65. Notably, prior to the 2017-2018 Data Breach, Defendants warranted the following to its customers: "Protecting the security of your information is very important to us . . . [o]nce we receive your transmission, we will take reasonable precautions to secure and protect the information on our systems."[49] As of the date of this Complaint, Defendants have altered this admission: "We have taken certain physical, administrative, and technical steps to safeguard the information we collect from and about our customers and Site visitors. While we make every effort to help ensure the integrity and security of our network and systems, we cannot guarantee our

[48] *Id*. at 38 (PCI DSS 3.2.1 and 3.2.2).
[49] Saks OFF 5TH Privacy Policy (April 11, 2016), https://web.archive.org/web/20160411092431/http:/www.saksoff5th.com/privacy-policy/privacy-policy.html?sre=terms_2 (last visited November 12, 2018)

security measures. When you enter sensitive information (such as credit card information) on our forms, we encrypt the transmission of that information using secure socket layer technology (SSL)."[50]

66. Despite Defendants' awareness of their data security obligations and their promises to customers that their personal data would be secured and protected, Defendants' treatment of Customer Data entrusted to them by their customers fell far short of satisfying Defendants' legal duties and obligations, and included violations of the PCI DSS. Defendants failed to ensure that access to their data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

D. Defendants Failed to Comply With FTC Requirements

67. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[51]

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[52] The guidelines note businesses should protect the personal customer

[50] Saks OFF 5th Privacy Policy (May 23, 2018), https://www.saksoff5th.com/main/static_content.jsp?pageId=stores-corporate-policy (last visited November 12, 2018)
[51] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited November 12, 2018).
[52] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited November 12, 2018).

information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

69. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[53]

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. In this case, Defendants were at all times fully aware of their obligation to protect the financial data of their customers because of their participation in payment card processing

[53] FTC, Start With Security, *supra* note 51.

networks. Defendants were also aware of the significant repercussions if they failed to do so because Defendants collect payment card data from tens of thousands of customers and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

73. Despite understanding the consequences of inadequate data security, Defendants failed to comply with PCI DSS requirements and failed to take additional protective measures beyond those required by PCI DSS.

74. Despite understanding the consequences of inadequate data security, Defendants operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect their data network.

E. Defendants' Data Breach

75. On information and belief, Defendants were put on notice several times regarding their lax data security.

76. Months before Fin7 successfully breached Defendants' security systems, Defendants was aware of their lax data-security standards. On March 17, 2017, BuzzFeed News notified HBC that the personal information of tens of thousands of Saks Fifth Avenue customers was publicly available online.[54] According to Robert Graham, cybersecurity expert and owner of Errata Security, "[t]his is bad as security gets … [e]veryone is vulnerable."[55] An HBC spokesperson responded that "[w]e take this matter seriously …[t]he security of our customers is

[54] Leticia Miranda, *Saks Fifth Avenue Exposed Personal Info on Tens of Thousands of Customers* (March 19, 2017), *available at* https://www.buzzfeed.com/leticiamiranda/saks-fifth-avenue-exposed-personal-info?utm_term=.navJN3B8E#.rrRG2Bpqr (last visited November 12, 2018).
[55] *Id.*

of utmost priority."[56] Once Defendants knew that their customers' personal information was exposed to the public, Defendants became aware, or should have become aware, that their data-security practices were insufficient.

77. On April 2017, one month following the March 2017 breach of its customer's personal data, HBC issued its Annual Information Form, admitting that "[a] potential privacy breach could have a material adverse effect on our business and results of operations."[57] HBC further recognized that "[o]ur security measures may be undermined due to the actions of outside parties, employee error, malfeasance, and, as a result, an unauthorized party may obtain access to our data systems and misappropriate business and personal information."[58] HBC was admittedly aware of the severe risks involved in a failure to maintain proper data security standards. Following the March 2017 breach of the personal information of tens of thousands of their customers, immediate action should have been taken to increase the pre-existing data security measures in place for Defendants' stores. Defendants failed to do so.

78. Following these events, on March 28, 2018, the hacking group known as Fin7 announced the breach of an unnamed major corporation, leading to the unauthorized access and disclosure of five million credit and debit cards. Fin7 previously carried out data breaches against Whole Foods, Chipotle, Omni Hotels & Resorts, and Trump Hotels.[59]

79. On April 1, 2018, Gemini Advisory, a cyber-threat research group working with several large financial institutions, became the first entity to report on the breach, confirming that

---

[56] *Id.*
[57] Hudson Bay Company, Annual Information Form, at 61 (Apr. 28, 2017).
[58] *Id.*
[59] Jackie Wattles, *Saks, Lord & Taylor breach: Data stolen on 5 million cards* (Apr. 1, 2018), *available at* http://money.cnn.com/2018/04/01/technology/saks-hack-credit-debit-card/index.html (last visited November 12, 2018).

the breach was linked to the HBC stores.[60] The breach of Defendants' systems allowed the thieves to extract customers' payment card information from approximately May 2017 to March 2018 for potentially all Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America.[61] According to Gemini's Chief Technology Officer, the hack "penetrated the retailers' point of sale systems."[62] As of April 1, 2018, approximately 125,000 payment card records have been released for sale, with Gemini experts "expect[ing] the entire cache to become available in the following months."[63]

80. On April 1, 2018, immediately following the Gemini Report, HBC confirmed that hackers breached and disclosed customer payment card data collected from its North American HBC stores.[64] HBC failed to provide consumers with any additional information regarding the scope or extent of the breach.[65] While HBC initially disclosed the data breach on the Saks OFF 5TH, Saks Fifth Avenue, and Lord & Taylor websites, the notices were taken down shortly thereafter.[66]

81. Following the breach, Mark Cline, Vice President of the data-security firm Netsurion, stated that "[t]his incident shows once again merchants still need to protect themselves against POS system infiltration attacks targeting cardholder data. A multi-layer security strategy

---

[60] Gemini Advisory, *supra* note 6.
[61] *Id*.
[62] Robert McMillan and Suzanne Kapner, *Saks, Lord & Taylor Hit With Data Breach* (Apr. 2, 2018), *available at* https://www.wsj.com/articles/saks-lord-taylor-hit-with-data-breach-1522598460 (last visited November 12, 2018).
[63] Gemini Advisory, *supra* note 6.
[64] Hudson's Bay Company, *http://investor.hbc.com/releasedetail.cfm?ReleaseID=1062423* (April 1, 2018) (last visited November 12, 2018).
[65] *Id.*
[66] No longer available at https://www.saksfifthavenue.com/main/static_content.jsp?pageId=security-information-notice&site_refer=EML; https://www.saksoff5th.com/security-information/notice.html; https://www.lordandtaylor.com/security-information/notice.html.

is necessary."[67] If such measures were in place, "[i]f nothing else, dwell time of such an attack would be reduced to hours or days."[68]

82. Despite Defendants' lax security standards and acknowledgement that their customers' personal information was valuable, the data breach occurred two months later, resulting from Defendants' acts and omissions in failing to properly protect Customer Data.

83. In addition to Defendants' failure to prevent the data breach, Defendants also failed to detect the breach for almost one year, only learning of the breach after the Gemini Report.[69]

84. The breach occurred because Defendants failed to implement adequate data security measures to protect their POS network from the potential danger of a data breach and failed to implement and maintain adequate systems to detect and prevent the breach and resulting harm that they have caused.

85. Had Defendants implemented and maintained adequate safeguards to protect the Customer Data, deter the hackers, and detect the data breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented.

86. In permitting the data breach to occur, Defendants breached their implied agreement with customers to protect their personal and financial information and violated industry standards.

---

[67] Teri Robinson, *Saks, Lord & Taylor breached, 5 million payment cards likely compromised* (Apr. 1, 2018), *available at* https://www.scmagazine.com/saks-lord-taylor-breached-5-million-payment-cards-likely-compromised/article/755180/ (last visited November 12, 2018).

[68] *Id.*

[69] Jim Finkle and David Henry, *Saks, Lord & Taylor hit by payment card data breach* (Apr. 3, 2018), *available at* https://www.reuters.com/article/legal-us-hudson-s-bay-databreach/saks-lord-taylor-hit-by-payment-card-data-breach-idUSKCN1H91W7 (last visited November 12, 2018).

F. The Data Breach Caused Harm and Will Result in Additional Fraud

87. Due to Defendants' failure to timely identify the breach, Fin7 was able to extract sensitive financial data from Defendants' customers for approximately one year. Customers, including Plaintiff and Class members, have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

88. The ramifications of Defendants' failure to keep Plaintiff's and Class members' data secure are severe.

89. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[70] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[71]

90. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[72]

91. Identity thieves can use personal information, such as that of Plaintiff and Class members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with

[70] 17 C.F.R § 248.201 (2013).
[71] *Id.*
[72] Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited November 12, 2018).

another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

92. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[73]

93. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[74]

94. There may be a time lag between when harm occurs versus when it is discovered, and also between when Customer Data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[75]

95. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred

[73] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited November 12, 2018).
[74] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited November 12, 2018).
[75] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited November 12, 2018).

by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

G. Plaintiff and Class Members Suffered Damages

96. Plaintiff's and Class members' Consumer Data is private and sensitive in nature and was left inadequately protected by Defendants. Defendants did not obtain Plaintiff's and Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

97. Defendants' Data Breach was a direct and proximate result of their failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

98. Defendants had the resources to prevent a breach, particularly considering the aforementioned expansions in Defendants' retail locations and investments in technology. Defendants neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.[76]

99. Had Defendants remedied the deficiencies in their POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Defendants would

[76] Mike Troy, *Surging Hudson's Bay Details Major Investments in Expanding Saks, Saks Off 5th and Store Renovation* (Apr. 5, 2016), *available at* https://www.chainstoreage.com/article/surging-hudsons-bay-details-major-investments-expanding-saks-saks-th-and-store-renovations/ (last visited November 12, 2018).

have prevented intrusion into their POS systems and, ultimately, the theft of their customers' confidential payment card information.

100. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

101. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of

Plaintiff's and Class members' Customer Information on the Internet card black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. money paid for goods purchased at Defendants' HBC Stores during the period of the Data Breach in that Plaintiff and Class members would not have shopped at Defendants' stores, or at least would not have used their payment cards for purchases, had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Defendants provided timely and accurate notice of the Data Breach;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their Customer Data, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the

amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

l. the loss of productivity and value of their time spent to address attempts to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

102. While the Plaintiff's and Class members' Consumer Data has been stolen, Defendants continue to hold Customer Data of consumers, including Plaintiff's and Class members'. Particularly because Defendants have demonstrated an inability to prevent a breach or detect it after running unhindered for approximately one year, Plaintiff and members of the Class have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ACTION ALLEGATIONS

103. Plaintiff seeks relief on behalf of herself and as the representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), Plaintiff seeks to certify a class of all persons residing in the United States who made a credit or debit card purchase at a Saks Fifth Avenue, Saks OFF 5TH or Lord & Taylor U.S. store from May 2017 to March 2018 (the "Nationwide Class").

104. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff also seeks to certify a class of all persons residing in California who made a credit or debit card purchase at a Saks Fifth Avenue, Saks OFF 5TH or Lord & Taylor California store from May 2017 to March 2018 (the "California Subclass").

105. The Nationwide Class and California Subclass are individually referred to as "Class" and collectively referred to as the "Classes."

106. Excluded from each of the Classes are Defendants and any of their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judges to whom this case is assigned as well as his or her judicial staff and immediate family members.

107. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

108. Plaintiff is a member of all Classes.

109. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

110. **Numerosity.** The proposed Classes include millions of customers whose data was compromised in the data breach. While the precise number of Class members has not yet been determined, the massive size of the data breach indicates that joinder of each member would be impracticable.

111. **Commonality and Predominance.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. Whether Defendants had a duty to protect Customer Data;

b. Whether Defendants knew or should have known of the susceptibility of their POS system to a data breach;

c. Whether Defendants' security measures to protect their POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other measures recommended by data security experts;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendants' failure to implement adequate data security measures allowed the breach of their POS systems to occur;

f. Whether Defendants' conduct constituted unfair, unlawful, and/or deceptive trade practices under California law;

g. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of the Customer Data of Plaintiffs and Class members;

h. Whether Defendants' breaches of their legal duties caused Plaintiff and the Class members to suffer damages;

i. Whether Defendants were negligent as a result of their possible violations of relevant statutes, as alleged herein.

j. Whether Plaintiff and Class members are entitled to recover damages; and

k. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

112. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of the claims of the Classes. Plaintiff and Class members were injured through Defendants' uniform misconduct and their legal claims arise from the same core practices employed or omitted by Defendants.

113. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiff is an adequate representative of the proposed Classes because her interests do not conflict with the interests of the Class members she seeks to represent. Plaintiff's counsel are experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive retail data breach cases.

114. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

115. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendants have acted or have refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

116. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to information regarding which of their stores were affected by the breach, the time period of the breach, which customers were potentially affected, as well as the addresses and other contact information for members of the Classes, which can be used for providing notice to the Class members.

COUNT I
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, PLAINTIFF AND THE CALIFORNIA SUBCLASS)

117. Plaintiff restates and realleges Paragraphs 1 through 116 as if fully set forth herein.

118. Defendants solicited and invited Plaintiff and Class members to shop at their retail stores and make purchases using their credit or debit cards. Plaintiff and Class members accepted Defendants' offers and used their credit or debit cards to make purchases at Defendants stores from May 2017 through March 2018.

119. When Plaintiff and Class members made and paid for purchases of Defendants' services and products from May 2017 through March 2018, they provided their Customer Data to Defendants. In so doing, Plaintiff and Class members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of their Customer Data.

120. Plaintiff and Class members would not have provided and entrusted their Customer Data with Defendants in the absence of the implied contract between them and Defendants.

121. Plaintiffs and Class members fully performed their obligations under the implied contracts with Saks.

122. Defendants breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect their Consumer Data and by failing to timely detect the data breach within a reasonable time.

123. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants, Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

COUNT II
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, PLAINTIFF AND THE CALIFORNIA SUBCLASS)

124. Plaintiff restates and realleges Paragraphs 1 through 116 as if fully set forth herein.

125. Upon accepting and storing the Plaintiff's and Class members' Customer Data in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Customer Data was private and confidential and should be protected as private and confidential.

126. Defendants owed a duty of care not to subject Plaintiff's and Class members' Customer Data to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

127. Defendants owed numerous duties to Plaintiff and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Customer Data in their possession;

b. to protect Customer Data using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

128. Defendants also breached their duty to Plaintiff and Class members to adequately protect and safeguard Customer Data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Customer Data. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Customer Data with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Customer Data of Plaintiff and Class members, misuse the Customer Data and intentionally disclose it to others without consent.

129. Defendants knew, or should have known, of the risks inherent in collecting and storing Customer Data, the vulnerabilities of POS systems, and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches within the retail industry, including their own security failures in the March 2017 public disclosure of customer's private information.

130. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' Customer Data.

131. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Customer Data.

132. Because Defendants knew that a breach of their systems would damage millions of their customers, including Plaintiff and Class members, Defendants had a duty to adequately protect their data systems and the Customer Data contained thereon.

133. Defendants had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Defendants with their Customer Data was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems, and the Customer Data they stored on them, from attack.

134. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Customer Data. Defendants' misconduct included failing to: (1) secure their point-of-sale systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

135. Defendants also had independent duties under state and federal laws that required them to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the data breach.

136. Defendants breached their duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' customer data;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Customer Data both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' customer data had been improperly acquired or accessed.

137. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Customer Data of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Customer Data during the time it was within Defendants' possession or control.

138. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the Customer Data to Plaintiff and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Customer Data.

139. Defendants breached their duty to notify Plaintiff and Class Members of the unauthorized access by not disclosing the breach as required by California's data breach law. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Plaintiff and the Class.

140. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiff's and Class members' Customer Data from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Customer Data during the time it was within Defendants' possession or control.

141. Further, through their failure to discover the breach for approximately one year, Defendants prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

142. Upon information and belief, Defendants improperly and inadequately safeguarded Plaintiff's and Class members' Customer Data in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect sensitive Plaintiff's and Class members' Customer Data, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the Customer Data.

143. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Customer Data; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' Customer Data; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Customer Data had been compromised.

144. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Customer Data as described in this Complaint.

145. As a direct and proximate cause of Defendants' conduct, Plaintiff and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the their Customer Data; damages arising from Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including, but not limited to, late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
VIOLATIONS OF THE CALIFORNIA DATA BREACH LAW (CAL. CIV. CODE SECTIONS 1798.81.5 & 1798.82)
(ON BEHALF OF PLAINTIFF AND THE CALIFORNIA SUBCLASS)

146. Plaintiff repeats the allegations contained in Paragraphs 1 through 116 above as if fully set forth herein.

147. Cal Civ. Code § 1798.81.5(a)(1) provides that its purpose is to "ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to

provide reasonable security for that information."

148. Cal. Civ. Code § 1798.81.5(b) provides, in pertinent part, that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

149. Under Cal Civ. Code § 1798.81.5(d)(1)(A)(i-iv), "personal information," as described in Cal Civ. Code § 1798.81.5(b), means the following:

> (A) [a]n individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
> (i) Social security number.
> (ii) Driver's license number or California identification card number.
> (iii) Account number, ***credit or debit card number***, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(emphasis added).

150. Therefore, the Customer Data disclosed in Defendants' Data Breach, which includes Plaintiff and Class members' credit and debit card information, combined with the necessary codes and/or passwords, falls within the meaning of "personal information" under Cal. Civ. Code Section 1798.81.5.

151. By failing to implement adequate and reasonable data security measures for this Customer Data, Defendants violated Cal. Civ. Code Section 1798.81.5.

152. Under Cal. Civ. Code Section 1798.82(a), businesses which conduct business in California and who own or license computerized data which include personal information are required to disclose breaches to California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person [. . .] [and] [t]he

disclosure shall be made in the most expedient time possible and without unreasonable delay."

153. Under Cal. Civ. Code Section 1798.82(d)(1), the disclosure must also "be written in plain language, shall be titled 'Notice of Data Breach,' and shall present the information [. . .] under the following headings: 'What Happened,' 'What Information Was Involved,' 'What We Are Doing,' 'What You Can Do,' and 'For More Information.'"

154. Because Defendants, as of the date of this Complaint, have not provided written notifications to California Residents as required under Cal. Civ. Code Section 1798.82(d)(1), Defendants continue to violate Cal. Civ. Code Section 1798.82(d)(1).

155. Because Defendants violated Cal. Civ. Code Sections 1798.81.5 and 1798.82, and continues to violate Cal. Civ. Code Section 1798.82, Plaintiff may seek an injunction pursuant to Cal. Civ. Code Section 1798.84(e), which states "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined." Specifically, Plaintiff seeks injunctive relief as follows -- Defendants must implement and maintain adequate and reasonable data security measures and abide by the California Data Breach laws, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems periodically, and ordering Defendants to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training their security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of Defendants' data security measures are compromised, hackers cannot gain access to other areas of Defendants' systems;

f. deleting, in a reasonable and secure manner, Personal Information not necessary for Defendants' provisions of services;

g. conducting regular database scanning and security checks;

h. issue security breach notifications to California Residents which abide by the requirements established under Cal. Civ. Code Section 1798.82(d);

i. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

j. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

COUNT IV
NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, FOR THE CALIFORNIA SUBCLASS)

On Behalf of the Nationwide Class

156. Plaintiff restates and realleges Paragraphs 1 through 116 as if fully set forth herein.

157. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Saks, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

158. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, and the foreseeable consequences of a data breach at an international retail chain as large as Defendants, including, specifically, the immense damages that would result to Plaintiff and Class members.

159. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

160. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

161. The harm that occurred as a result of the Defendants' Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

162. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including, but not limited to, late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

On Behalf of the California Subclass

163. Plaintiff restates and realleges Paragraphs 1 through 116 as if fully set forth herein.

164. Section 1798.81.5(b) of the California Civil Code establishes that any "business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

165. Defendants violated Section 1798.81.5(b) of the California Civil Code by failing to implement and maintain reasonable security procedures and practices necessary to protect Plaintiff and Class members' private information from unauthorized access, particularly considering their earlier failure to safeguard their customers' private information.

166. Defendants' violation of Section 1798.81.5(b) of the California Civil Code thereby constitutes negligence per se.

167. Plaintiff and Class members are within the class of persons that California Civil Code Section 1798.81.5(b) was intended to protect because they are California residents.

168. The harm which occurred due to Defendants' Data Breach is the type of harm that California Civil Code Section 1798.81.5(b) was intended to protect. Specifically, this is the harm of the unauthorized access or disclosure of personal information due to a failure to maintain reasonable security procedures.

169. Therefore, the harm that occurred as a result of Defendants' Data Breach is the type of harm Section 1798.81.5(b) of the California Civil Code was created to protect.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, PLAINTIFF AND THE CALIFORNIA SUBCLASS)

170. Plaintiff restates and realleges Paragraphs 1 through 116 as if fully set forth here.

171. Plaintiff and Class members conferred a monetary benefit on Saks. Specifically, they purchased goods and services from Defendants and provided Defendants with their payment information. In exchange, Plaintiff and Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Customer Data with adequate data security.

172. Defendants knew that Plaintiff and Class members conferred a benefit on HBC and accepted and has accepted or retained that benefit. Defendants profited from their purchases and used Plaintiff's and Class members' Customer Data for business purposes.

173. Defendants failed to secure Plaintiff's and Class members' Customer Data and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' Customer Data provided.

174. Defendants acquired the Customer Data through inequitable means as they failed to disclose the inadequate security practices previously alleged.

175. If Plaintiff and Class members knew that Defendants would not secure their Customer Data using adequate security, they would not have made purchases at Defendants' stores.

176. Plaintiff and Class members have no adequate remedy at law.

177. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

178. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT VI
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, PLAINTIFF AND THE CALIFORNIA SUBCLASS)

179. Plaintiff restates and realleges Paragraphs 1 through 116 as if fully set forth here.

180. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this Complaint.

181. As previously alleged, Plaintiff and Class members entered into an implied contract that required Defendants to provide adequate security for the Customer Data they collected from their payment card transactions. As previously alleged, Defendants owe duties of care to Plaintiff and Class members that require it to adequately secure Customer Data.

182. Defendants still possess Customer Data pertaining to Plaintiff and Class members.

183. Defendants have made no announcement or notification that it has remedied the vulnerabilities in their computer data systems, and, most importantly, their POS systems.

184. Accordingly, Defendants have not satisfied their contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Defendants' lax approach towards data security has become public, the Customer Data in their possession is more vulnerable than previously.

185. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

186. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' Customer Data and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Defendants' existing data security measures do not comply with their legal duties of care;

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' Customer Data.

187. Plaintiff also requests an injunction requiring Defendants to comply with their contractual obligations and duties of care and implement and maintain reasonable security measures, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems periodically, and ordering Defendants to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement[ing] and maintain[ing] reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training their security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of Defendants' data security measures are compromised, hackers cannot gain access to other areas of Defendants' systems;

f. deleting, in a reasonable and secure manner, Personal Information not necessary for Defendants' provisions of services;

g. conducting regular database scanning and security checks;

h. issuing security breach notifications to California Residents which abide by the requirements established under Cal. Civ. Code Section 1798.82(d);

i. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

j. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

188. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event Defendants incur another data breach. The risk of another such breach is real, immediate, and substantial.

189. The hardship to Plaintiff and other customers if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. If Defendants incur another data breach, Plaintiff and other customers will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

190. Such an injunction would benefit the public by preventing another data breach for Defendants, and therefore eliminating the additional injuries that would result to Plaintiff and the millions of customers whose confidential information would be further compromised.

COUNT VII
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL"), CALIFORNIA BUSINESS & PROFESSIONS CODE §§ 17200, *ET SEQ.*
(ON BEHALF OF PLAINTIFF AND THE CALIFORNIA SUBCLASS)

191. Plaintiff repeats the allegations contained in Paragraphs 1 through 116 above as if fully set forth herein.

192. UCL § 17200 provides, in pertinent part, that "unfair competition shall mean and include unlawful, unfair, or fraudulent business practices [. . .]".

193. Under the UCL, a business act or practice is "unlawful" if the act or practice violates any established state or federal law.

194. Defendants' failures to implement and maintain reasonable security measures and to timely and properly notify Plaintiff and Class members of the data breach therefore was and continues to be "unlawful" as Defendants breached their implied and express warranties and violated the California law regarding data breaches, specifically California Code of Civil Procedure Sections 1798.81.5(b) and 1798.82, as well as Section 5 of the FTC Act.

195. As a result of Defendants' unlawful business acts and practices, Defendants unlawfully obtained money from Plaintiff and members of the Class.

196. Under the UCL, a business act or practice is "unfair" if the defendant's conduct is substantially injurious to consumers, goes against public policy, and is immoral, unethical, oppressive, and unscrupulous, as the benefits for committing these acts or practices are outweighed by the severity of the harm to the alleged victims.

197. Here, Defendants' conduct was and continues to be of no benefit to their customers, as it is both injurious and unlawful to those persons who rely on Defendants' duties and obligations to maintain and implement reasonable data security measures and to monitor for breaches. Having lax data security measures that has resulted in the disclosure of millions of customers' payment

card information provides no benefit to consumers. For these reasons, Defendants' conduct was and continues to be "unfair" under the UCL.

198. As a result of Defendants' unfair business acts and practices, Defendants have unfairly and unlawfully obtained money from Plaintiff and members of the Class.

199. Further, Defendants have fraudulently omitted material information in violation of the UCL by failing to disclose their inadequate data security measures, which was material to consumers as they would not have purchased items from HBC's stores had Defendant disclosed the information. Further, Defendants had a duty to disclose this information to Plaintiff and members of the California Subclass based on the factual allegations discussed herein, which demonstrate the following: (1) Defendants, Plaintiff, and California Subclass members were in a special relationship arising from Defendants' role in safeguarding consumers' sensitive consumer data; (2) Defendants held exclusive knowledge of the material facts surrounding their inadequate data security measures, which were not known to Plaintiff and class members; and (3) Defendants made a partial misrepresentation when warranting on their website that customers' private data would be secured, suppressing the material fact that their data security measures were inadequate.

200. Plaintiff requests that this Court enjoin Defendants from violating the UCL or violating the UCL in the same way in the future, as discussed herein. Otherwise, Plaintiff and members of the Class may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

201. Plaintiff re-alleges and incorporates by reference each preceding paragraph as though set forth at length herein.

COUNT VIII
VIOLATION OF MISSISSIPPI'S CONSUMER PROTECTION ACT UNFAIR COMPETITION LAW ("MCPA"),
Miss. Code §§ 75-24-1, *et seq*.
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

202. Plaintiff repeats the allegations contained in Paragraphs 1 through 116 above as if fully set forth herein.

203. Defendants are "person[s]," as defined by Miss. Code § 75-24-3.

204. As further discussed in Paragraph 31 Defendants advertised, offered, or sold goods or services Nationwide, including in Mississippi, and engaged in trade or commerce directly or indirectly affecting the people Nationwide, including in Mississippi, as defined by Miss. Code § 75-24-3.

205. Defendants engaged in unfair and deceptive trade acts or practices, including:

a. failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' customer data;

b. creating a foreseeable risk of harm through the misconduct previously described;

c. failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Customer Data both before and after learning of the Data Breach;

d. failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. failing to timely and accurately disclose that Plaintiff's and Class members' customer data had been improperly acquired or accessed.

206. The above-described conduct violated Miss. Code § 75-24-5(2), including:

a. Representing that goods or services have sponsorship, approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

207. Defendants intended to mislead and induce Plaintiff and Class members into relying on Defendants' misrepresentations and omissions regarding their data security.

208. Defendants' misrepresentations and omissions were material as they were likely to deceive reasonable consumers into believing that Defendants maintain adequate data security measures and were able to adequately safeguard the Customer Data.

209. Had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard the Customer Data, Plaintiff and Class members would not have shopped with Defendants or would not have used their payment cards at Defendants' HBC stores. However, because Defendants failed to disclose this information and Plaintiffs and Class members had no reasonable method of discovering the truth of the information, Plaintiff and Class members were reasonable in relying on Defendants' ability to safeguard the Customer Data.

210. Defendants carried a duty to disclose the data breach due to, *inter alia*, the sensitivity of the Customer Data they possessed, their knowledge of previous data breaches suffered by HBC stores and other businesses, Plaintiff and Class members' inability to adequately protect their Customer Data once provided to Defendants' and their data security features, the professional standards expected of them, and the numerous legal, ethical requirements mandating they make such disclosures.

211. For the reasons discussed above, Defendants acted intentionally, knowingly, and maliciously in violating the MCPA. In doing so, Defendants recklessly disregarded the rights of Plaintiff and the Class Members.

212. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting data breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the data breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

213. Plaintiff, Class members, and the general public continue to suffer a present and future risk of harm from Defendants' actions and omissions.

214. Under Miss. Code § 75-24-11, Plaintiff seeks monetary damages, including but not limited to actual and restitutionary damages, injunctive relief, punitive damages, and reasonable attorneys' fees, expenses and costs of suit.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants as follows:

a) For an order certifying the Nationwide Class and the California Subclass under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiff as representative of all Classes; and naming Plaintiff's attorneys as Class Counsel to represent all Classes;

b) For an order declaring that Defendants' conduct violates the statutes and laws

referenced herein;

c) For an order finding in favor of Plaintiff, and all Classes, on all counts asserted herein;

d) For an order awarding all damages in amounts to be determined by the Court and/or jury;

e) For prejudgment interest on all amounts awarded;

f) For interest on the amount of any and all economic losses, at the prevailing legal rate;

g) For an order of restitution and all other forms of equitable monetary relief;

h) For injunctive relief as pleaded or as the Court may deem proper;

i) For an order awarding Plaintiff and all Classes their reasonable attorneys' fees, expenses and costs of suit, including as provided by statute such as under the Federal Rules of Civil Procedure 23(h); and

j) For any other such relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: November 12, 2018

FARUQI & FARUQI, LLP

By: */s/ Nina Varindani*
Nina Varindani (NV-1090)
685 Third Avenue, 26th Fl.
New York, NY 10017
Telephone: 212-983-9330
Fax: 212-983-9331
Email: nvarindani@faruqilaw.com

Timothy J. Peter (*pro hac vice*)
1617 JFK Boulevard, Suite 1550
Philadelphia, PA 19103

Telephone: (215) 277-5770
Fax: (215) 277-5771
E-mail: tpeter@faruqilaw.com

Benjamin Heikali (*pro hac vice*)
10866 Wilshire Blvd., Suite 1470
Los Angeles, CA 90024
Telephone: 424.256.2884
Fax: 424.256.2885
E-mail: bheikali@faruqilaw.com

Attorneys for Plaintiffs